PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-190795
(43)Date of publication of application : 05.07.2002

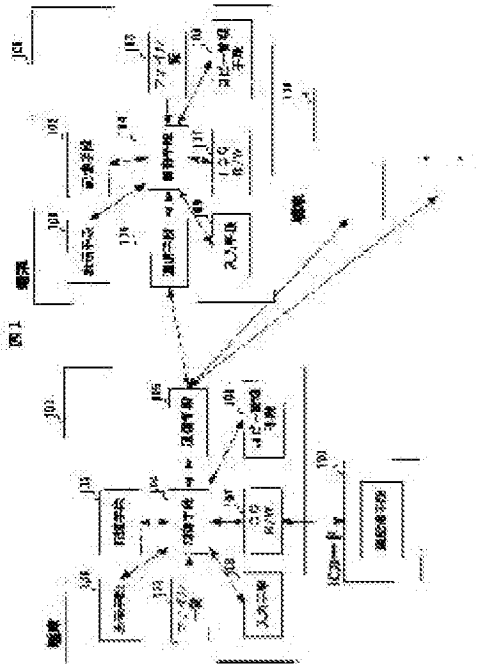
(51)Int.Cl. H04L 9/08
G06F 12/00
G06F 12/14
G06F 13/00
H04L 9/10

(21)Application number : 2000-391826
(22)Date of filing : 20.12.2000

(71)Applicant : HITACHI LTD
(72)Inventor : YAMAUCHI TOMOMI
INOUE YOSHITAKE
NAKADE MAYUMI
TAKAMI MINORU
ITO SHIGEYUKI

(54) INFORMATION TERMINAL AND INFORMATION TERMINAL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To temporarily share digital contents data by a plurality of terminals while preventing digital contents from being illegally copied.
SOLUTION: Ciphered digital contents, a key to be used for the decoding of the ciphered digital contents and a copying condition file are transmitted from a 1st terminal to a 2nd terminal. The 2nd terminal decodes the digital contents by referring to the received copying condition file, and after the end of decoding processing, deletes the key used for the decoding.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－190795
（P2002－190795A）
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	12/00	５３７Ｈ　５Ｂ０１７
Ｇ０６Ｆ	12/00	５３７		12/14	３２０Ｂ　５Ｂ０８２
	12/14	３２０			３２０Ｅ　５Ｊ１０４
				13/00	５４０Ｓ
	13/00	５４０	Ｈ０４Ｌ	9/00	６０１Ｂ

審査請求　未請求　請求項の数10　ＯＬ　（全 ７ 頁）　最終頁に続く

(21)出願番号　特願2000－391826(P2000－391826)

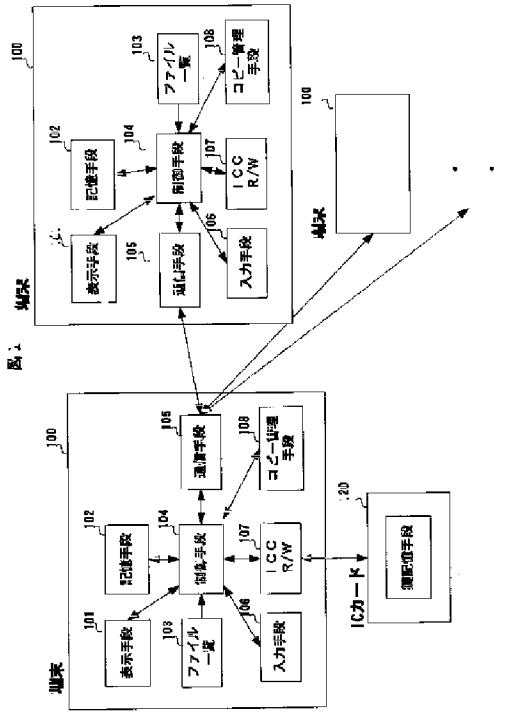
(22)出願日　平成12年12月20日(2000.12.20)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　山内　伴美
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　井上　喜勇
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　情報端末及び情報端末システム

(57)【要約】
【課題】デジタルコンテンツの不正コピーを防ぎつつも、複数の端末における一時的なデジタルコンテンツデータの共有を実現する。
【解決手段】第一の端末から第二の端末に、暗号化されたデジタルコンテンツ、暗号化されたデジタルコンテンツの復号化に用いる鍵、コピー条件ファイルを送信する。第二の端末においては、受信したコピー条件ファイルを参照に、デジタルコンテンツの復号化を行い、復号化処理終了後は復号化に用いた鍵を削除する。



【特許請求の範囲】
【請求項１】外部記憶手段に記憶された鍵情報を読み取り可能な情報端末であって暗号化されたコンテンツデータを記憶する記憶手段と、
該記憶手段に記憶された該コンテンツデータを復号化するコピー管理手段と、
該復号化されたコンテンツデータを表示する表示手段と、
該表示手段に表示されたコンテンツデータのファイル一覧から所望のファイルを選択指示する入力手段とを有し、
前記コピー管理手段は、前記入力手段により選択された前記ファイルのセキュリティ属性に応じて、前記外部記憶手段から読み出した鍵情報を前記記憶手段に記憶し、前記記憶手段に記憶した鍵情報を用いて前記ファイルのデータを復号し、前記表示手段に復号化された前記コンテンツデータを表示させ、前記記憶手段に記憶した鍵情報を削除することを特徴とする情報端末。
【請求項２】請求項１に記載の情報端末において、
他の情報端末と通信する通信手段を設け、
前記入力手段により所望のファイルが選択され、該選択されたファイルのコピー条件が入力されたときに、前記コピー管理手段が、前記入力手段により入力された前記選択ファイルのデータと、前記コピー条件と、前記外部記憶手段に記憶した鍵情報を前記他の情報端末に送信するよう前記通信手段を制御することを特徴とする情報端末。
【請求項３】請求項２に記載の情報端末において、
前記選択されたファイルのデータを前記他の端末に送信した際に、送信先の前記他の情報端末に送信した履歴情報を記憶する送信先履歴記憶手段とを備えたことを特徴とする情報端末。
【請求項４】請求項１又は２に記載の情報端末において、
他の情報端末から送信された選択ファイルのデータとファイルのコピー条件と鍵情報を受信する通信手段を設け、
前記他の情報端末から受信したデータを前記記憶手段に記録し、受信したコピー条件に基づいて受信した鍵情報を用いて受信したファイルの復号化を行い、前記表示手段に復号化されたファイルのデータを表示させ、前記受信したコピー条件に基づいて前記復号化ファイルを処理することを特徴とする情報端末。
【請求項５】請求項４に記載の情報端末において、
前記他の端末から送信された前記鍵情報を、揮発性の記憶手段に格納することを特徴とする情報端末。
【請求項６】請求項４又は５に記載の情報端末において、
前記受信したファイルを復号する際に、前記情報端末の端末ＩＤ及びパスワードのうち少なくとも一つを使用することを特徴とする情報端末。
【請求項７】請求項２乃至６のいずれか１項に記載の情報端末において、
前記コピー条件は、コピー先において復号化データを表示する回数及び時間及び複製したデータの再コピーの可否及び印刷の可否及び複製したデータを復号するときに必要なパスワード及び複製先の端末ＩＤ及びコピー先記憶手段の特性のデータのうちいずれか１つを含むことを特徴とする情報端末。
【請求項８】請求項１乃至７のいずれか１つに記載の情報端末おいて、
前記外部記憶手段はＩＣカード又はメモリーカードであることを特徴とする情報端末。
【請求項９】請求項１に記載の情報端末を第１の情報端末と第２の情報端末として有する情報端末システムであって、
前記第１の情報端末及び第２の端末装置に、情報端末間で通信する通信手段を設け、
前記第１の情報端末は、前記入力手段により所望のファイルが選択され、該選択されたファイルのコピー条件が入力されたときに、前記コピー管理手段が、前記入力手段により入力された前記選択ファイルのデータと前記コピー条件と、前記外部記憶手段に記憶された鍵情報を第２の情報端末に送信するよう前記通信手段を制御し、
前記第２の端末は、前記第１の端末から受信したデータを記憶手段に記録し、受信した前記コピー条件に基づいて受信した鍵情報を用いて受信したファイルの復号化を行い、前記第２の端末の表示手段に表示し、前記第２の端末のコピー管理手段は、前記コピー条件に基づいて復号化後のファイルを処理することを特徴とする情報端末システム。
【請求項１０】請求項９に記載の情報端末システムにおいて、
前記第１の端末から前記第２の端末に送信する選択ファイルのデータとファイルのコピー条件と鍵情報は、前記第１の端末において暗号化され、前記第２の端末で受信した際に復号化されるデータであることを特徴とする情報端末システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信手段を備えた携帯端末に係わり、複数の携帯端末間におけるデータ共有を実現するものである。
【０００２】
【従来の技術】従来のデジタルコンテンツの形態としては、自由にコピーが許されているコンテンツや著作権の管理されたコンテンツなど、様々なセキュリティ属性のコンテンツが存在する。著作権の管理されたコンテンツに関しては、コピープロテクションがかかっていたりしてコピー管理が厳しく、ユーザは自由にコピーすること

が許されなかった。

【０００３】

【発明が解決しようとする課題】デジタルコンテンツのコピーを無制限に認めることはできないが、完全にコピーを禁止すると、例えば会議などにおいて内輪でコンテンツデータを参照したい場合等は不便である。会議などでコンテンツを見たい場合、携帯端末の画面を複数人で参照するのは難しいが、著作料を支払ってまでコンテンツデータを全員にコピーするほどではない場合があり、コピーが完全に禁止されるのは不便である。

【０００４】本発明は、不正使用を防ぎながらも、複数の携帯端末間における一時的なコンテンツデータ共有の実現を目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明では、通信手段を備えた情報端末及び暗号化を解く鍵を格納した外部記憶手段を設け、情報端末に記録された暗号化データを参照する際に、外部記憶手段に記録した暗号化を解くための鍵を、一旦情報端末の記憶手段にコピーし、そのコピーした鍵を用いて一回限りデータを復号する構成とする。

【０００６】複数の携帯端末で参照する際には、オリジナルのコンテンツの鍵を各情報端末の記憶手段にコピーし、各自が、例えば一度限り、２時間限りなどの制限を伴って、コピーしたコンテンツを参照する。

【０００７】

【発明の実施の形態】以下、本発明の各実施例を図面を用いて説明する。なお、各実施例の図における同一符号は同一物または相当物を示し重複する説明は省略する。

【０００８】図1は本発明の情報端末システムであるデータシェアリングシステムの第１実施例のブロック構成図である。本発明の第１実施例におけるデータシェアリングシステムは、図１に示すように、情報端末100と外部記憶手段であるＩＣカード120から成り、端末100、表示手段101、記憶手段102、ファイル一覧103、制御手段104、通信手段105、入力手段106、ICCR/W107、コピー管理手段108を備え、ＩＣカード120は、鍵記憶手段121を備える。

【０００９】ＩＣカード120に記録した鍵は、例えば暗号化されたコンテンツデータの読み出しを行う際に、暗号化したデータを復号化するのに用いる。ＩＣカード120からの鍵の読み出しには認証を必要とするので、暗証番号を知っている人しか鍵の読み出しは行えない。

【００１０】なお、本実施例においては外部記憶手段としてはＩＣカードを用いたが、その他の記憶手段を用いてもよい。

【００１１】次に、図２を用いて、端末100内の暗号化データを読み出す際のフローを説明する。なお、図２におけるフローは、コンテンツの暗号鍵が記憶されたＩＣカードを有する端末ユーザーのフローである。ステップ201において、ユーザは、表示手段101に表示された端末100内の記憶手段102に格納されたファイル一覧103から、参照したいコンテンツデータのファイルを選択する。

【００１２】次に、ステップ202において、端末100のコピー管理手段108は、ユーザの選択したファイルのセキュリティ属性を参照する。

【００１３】ステップ203において、端末100のコピー管理手段108は、ユーザの選択したコンテンツデータの復号化には鍵が必要かどうか確認する。

【００１４】鍵が必要である場合には、ステップ204において、端末100の制御手段104又はコピー管理手段108はＩＣカード120に記録された鍵を端末100の記憶手段102に複製する。つまり、ＩＣカード120に記録された鍵を読み出して、記憶手段102に記憶させることにより鍵の複製（鍵のコピー）を行う。

【００１５】ステップ205において、端末100のコピー管理手段108は、端末100の記憶手段102にコピーした鍵を用いてデジタルコンテンツデータの復号化処理を行う。

【００１６】ステップ206において、端末100のコピー管理手段108は、コンテンツデータの復号化処理終了後、端末100の記憶手段102から鍵を削除する。

【００１７】ステップ207において、制御手段104又はコピー管理手段10はコンテンツデータを表示手段101に表示する。

【００１８】ステップ203において、コンテンツデータの復号に鍵が必要でない場合は、そのままステップ207に進み、制御手段104又はコピー管理手段はコンテンツデータを表示手段101に表示する。

【００１９】なお、端末装置内の記憶手段の鍵は削除することを説明したが、ＩＣカードに記憶された暗号鍵はそのまま保持させる構成としてもよい。また、端末装置100の記憶手段102に暗号鍵が複製された際(ステップ２０４)や端末の記憶手段から暗号鍵を削除する際（ステップ206）に削除する、あるいは、端末装置側にコンテンツが再生済みであることを記憶させ、再度の暗号鍵のコピーを禁止する、あるいは、既に暗号鍵が複製済みであることをＩＣカードに記憶させる、等の構成をとってＩＣカードに記憶された暗号鍵を用いて同じコンテンツを再度再生することができない構成としてもよい。

【００２０】図３は、端末100の記憶手段102に格納したデジタルコンテンツを、他の端末100にコピーする際のフローを示す。

【００２１】ステップ301において、オリジナルのコンテンツデータを持つユーザは、表示手段101に表示された端末100内のファイル一覧103から、コピーするコンテンツデータを選択する。

【００２２】ステップ302において、ユーザはコンテンツデータのコピー条件を入力手段106により入力する。

【００２３】ステップ303において、端末100のコピー管

理手段108は、コピー条件がセキュリティ属性を満足しているかどうか確認する。満足している場合には、端末100のコピー管理手段108は、ステップ304において、コピー元の端末100とコピー先の端末100同士の端末間認証を確認する。この場合の認証とは、例えば、端末ＩＤやパスワード等によつ通信先確認をさす。

【００２４】図４に、セキュリティ属性データを示す。セキュリティ属性データは、ファイル名に対応した、“コピーフリー”、“暗号鍵有”等のファイルのセキュリティ属性を示す。“コピーフリー”とは、ファイルが自由にコピー可能であることをセ示す。“暗号鍵有”は、ファイルが暗号化されているのでデータの読み出しに暗号鍵が必要であることを示す。

【００２５】次に、ステップ305において、端末100のコピー管理手段108はコンテンツデータと暗号鍵とコピー条件ファイルをコピー先端末100の記憶手段102に送信する。なお、この際に送信元端末100の不図示の送信先履歴記憶手段に、コピー先端末100に記録したことを示す履歴情報を記憶させてもよい。コピー先端末を記憶させることにより、コピーの管理を行うことができる。

【００２６】ステップ306において、コピー先の端末100のコピー管理手段108は、コピー条件ファイルを参照に、コンテンツデータと共に受信した鍵を用いてデジタルコンテンツを復号化する。

【００２７】ステップ307において、コピー先の端末100のコピー管理手段108は、コンテンツデータの復号化処理後、記憶手段102に記憶した鍵を削除する。

【００２８】ステップ308において、コピー先の端末100の制御手段104又はコピー管理手段108は、復号化したデジタルコンテンツを表示手段101に表示する。

【００２９】次に、図５を用いて、コンテンツデータを他の端末100にコピーする際の端末100の画面推移を説明する。

【００３０】図４は、コンテンツデータのセキュリティ属性データを示す。例えば、Ａ．ＦＩＬＥという名前のコンテンツデータのセキュリティ属性は、コピーフリーであるので、自由に他の端末100にコピー可能であることを示す。また、Ｂ．ＦＩＬＥという名前のファイルのセキュリティ属性は、コピーフリーであり、「暗号鍵有」なので、暗号化されたフォーマットであることを示す。また、Ｃ．ＦＩＬＥという名前のファイルのセキュリティ属性は、コピー不可で、かつ、暗号化されたフォーマットであることを示す。図には示していないが、権利の回数買いなど、その他様々なセキュリティ属性のコンテンツデータを扱ってもよい。なお、他人には見せられないデータに、秘密データであることを示す属性データを持たせてもよい。このような秘密データの場合は、コピー管理手段が、コピーを許可する他の端末のみへのコピーを行わせることとする。また、コピー先において復号化データを表示する回数、時間、印刷の可否、複製したデータを復号するときに必要なパスワード、複製先の端末ＩＤ、コピー先記憶手段の特性のデータを属性データとしてもよい。

【００３１】次に、図５を用いてユーザが自分の端末100のコンテンツデータを他の端末100にコピーする際に、端末100が表示する画面推移を説明する。

【００３２】まず、ファイル一覧103画面において、ユーザはコピーしたいファイルを選択する。

【００３３】例えば、ユーザがＢ．ＦＩＬＥを選択した場合、端末100の制御手段104は、表示手段101に、コピー条件を入力する画面を表示する。例えば、Ｂ．ＦＩＬＥとい名前のファイルであるコンテンツデータを、端末ＩＤが“００２７３”である端末にコピーするとして、パスワードは“＊＊＊＊”と設定し、その他ファイル属性等を設定する。RWXは、ファイルの、R(読みだし)、W(書き込み)、X(実行)が可能であるかどうかの属性を示す。

【００３４】ユーザがコピーしたいファイルを選択した場合に、端末100の制御手段104がコンテンツデータのセキュリティ属性を確認し、選択したファイルがコピー不可であった場合には、制御手段104は、「ユーザの選択したファイルのセキュリティ属性ははコピー不可である」という旨のメッセージを表示する。また、同時に、「著作料を支払えばコピー可能」等の、現状コピー不可であるデジタルコンテンツをコピーするための手段を提示してもよい。また、選択したファイルが秘密ファイルであるときは、「コピーを許可するか否か？」を表示手段101に表示させ、ユーザーが入力手段106により許可か不許可を入力し、これに従って、コピーするか否かを決定する。

【００３５】本実施例においてはコピー条件としては鍵寿命を定めているが、その他、データを複製可能な回数や、表示手段101に表示しておける時間の制限データや、その他データを複製するときに必要なパスワード等を定めてもよい。また、パスワードとしては、何度も利用できるもののみでなく、一回限り有効なパスワードを使用してもよい。また、その他コピー条件としては、複製データの再複製の可否や、印刷の可否等の詳細情報を定めても良い。

【００３６】次に、図６を用いて、コピー先端末でのフローを説明する。

【００３７】コンテンツデータと鍵のコピーとコピー条件ファイルを受信した端末におけるフローを説明する。

【００３８】ステップ601において、コピー先端末の制御手段104は、通信手段105経由でコンテンツデータと鍵のコピーとコピー条件ファイルを受け取る。

【００３９】ステップ602において、端末は受信したコピー条件を表示手段101に提示し、ユーザはパスワードを入力手段106により入力する。

【００４０】ステップ603において、パスワードが一致

した場合には、ステップ604において、コピー管理手段108は、鍵データを復号化する。ユーザの入力したパスワードが一致しなかった場合には、ステップ608においてコピー管理手段は、コンテンツデータ、鍵データを削除する。

【００４１】次に、ステップ605において、コピー管理手段108は、ステップ604において復号化した鍵を用いてコンテンツデータを復号化する。

【００４２】次に、ステップ606において、コピー管理手段108は、コンテンツデータの復号化処理終了後、記憶手段に記憶された鍵を削除し、ステップ607において制御手段104又はコピー管理手段108が復号したデジタルコンテンツを表示手段に表示する。

【００４３】なお、本実施例では、コピー条件としてコピー先端末ＩＤ及びパスワード等の情報を指定しているが、どちらか一方、またその他の情報を指定して、不正コピー防止を目的としたユーザの認証に用いてもよい。

【００４４】また、本実施例では、コピー先端末において受信データのうち少なくとも鍵データは、データ復号化終了後に削除しているが、あらかじめデータを記録する際に、ＤＲＡＭやＳＲＡＭ等の電源が落ちるとデータが消える特性である記憶手段に格納してもよい。また、ユーザが記憶手段を選択する手段をさらに備えてもよいし、自動的に揮発性の記憶手段に記録してもよい。

【００４５】また、本実施例においては、コピー先端末では、一旦受信データを記録しているが、データを記録せずに、復号化したデータを表示するのみにしてもよい。

【００４６】なお、上記の実施例においては、コピー管理手段と制御手段とを分けて説明したが、CPUがコピー管理手段と、制御手段の両方の役割を果たしてもよい。また、コピー管理手段と、制御手段の機能を果たすためのプログラムを不図示の記憶手段に記憶させておき、このプログラムに従ってCPUが動作させる構成としてもよい。

【００４７】

【発明の効果】本発明によれば、情報端末において、不正利用を防ぐことができる。また、複数の情報端末間で、デジタルコンテンツの一時的データ共有を実現することができる。

【図面の簡単な説明】

【図１】本発明のシステムのブロック構成図である。

【図２】コンテンツデータを再生する際のフロー図である。

【図３】コンテンツデータを端末間でコピーする際のフロー図である。

【図４】セキュリティ属性データの説明図である。

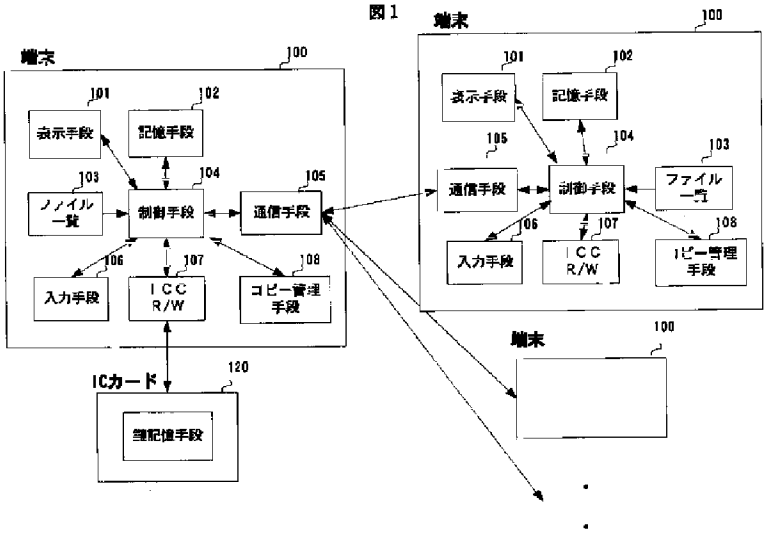
【図５】コンテンツデータをコピーする際の端末の画面推移を示す図である。

【図６】コンテンツデータをコピーした端末のフロー図である。

【符号の説明】

100…端末、101…表示手段、102…記憶手段、103…ファイル一覧、104…制御手段、105…通信手段、106…入力手段、107…ＩＣカードR/W、108…コピー管理手段、120…ＩＣカード

【図１】



【図４】

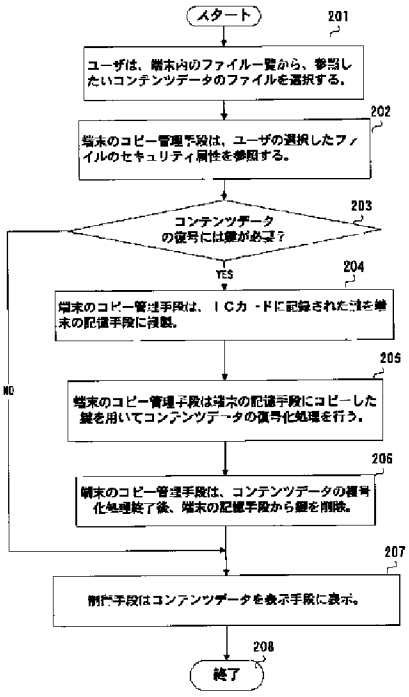
図4

セキュリティ属性データ

ファイル名	セキュリティ属性		
	コピーフリー	暗号鍵有	・
A. FILE	○	×	・
B. FILE	○	○	・
C. FILE	×	○	・
・	・	・	・

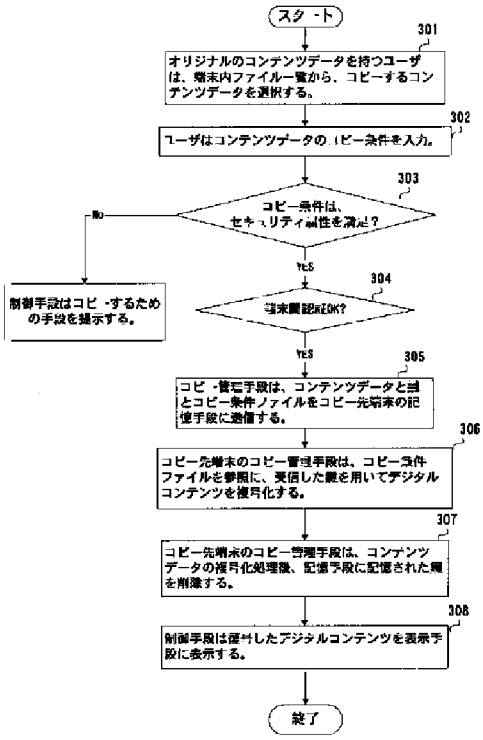
【図2】

図 2



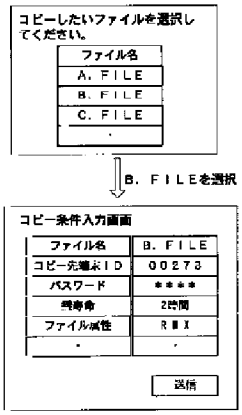
【図3】

図 3



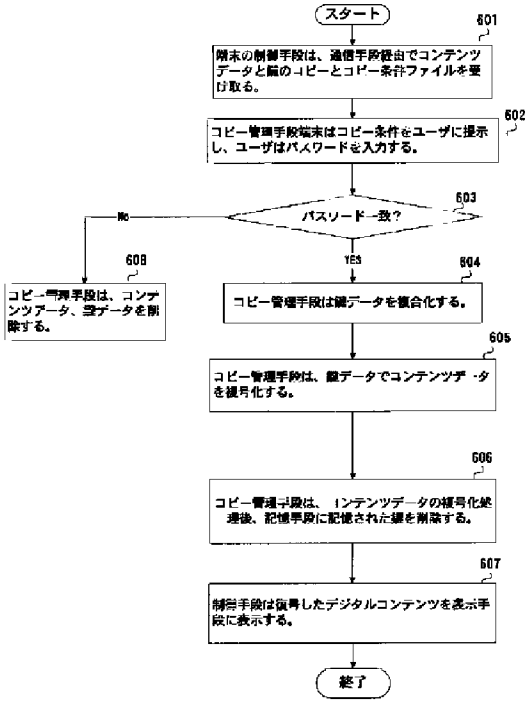
【図5】

図 5



【図6】

図 6



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
H04L 9/10		H04L 9/00	621A

(72)発明者 中出 真弓
神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内
(72)発明者 高見 穣
神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内
(72)発明者 伊藤 滋行
神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

Fターム(参考) 5B017 AA07 BA07 CA16
5B082 EA11
5J104 AA01 AA16 EA04 EA16 EA26 NA02 NA05 NA35 NA37 PA02 PA07